REMARKS

These remarks are set forth in response to the Office Action. As this amendment has been timely filed within the three-month statutory period, neither an extension of time nor a fee is required. Presently, claims 1 through 17 are pending in the Patent Application. Claims 1, 3, 8, 11 and 16 are independent claims. In paragraphs 1 and 2 of the Office Action, claims 1 through 5, 7 through 13 and 15 through 17 have been rejected under 35 U.S.C. § 102(e) as being anticipated by United States Patent No. 6,779,033 to Watson et al. (Watson). Also, in paragraph 3, claims 6 and 14 have been objected to only in that each depends upon a rejected base claim. The Examiner has indicated that claims 6 and 14 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

In response, the Applicants respectfully traverse the rejections on the art as the Applicants believe that Watson alone cannot support a prima facie case of anticipation as required under the Patent Act and defined in the Manual of Patent Examining Procedure (MPEP), section 2131. In this regard, MPEP section 2131 states, "A claim is anticipated *only if each and every element as set forth in the claim is found*, either expressly or inherently described in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628 (Fed. Cir. 1987). In the instant case, the Applicants contend that claimed elements in each of the independent claims cannot be found in the Watson reference.

Prior to a more in depth discussion of the rejections on the art, however, a brief review of the Applicants' invention is appropriate. The Applicants have invented a novel and non-obvious method and system for protecting a privately-accessible network from SYN and ACK flood attacks and from unauthorized intrusions based upon quasi-TCP connections with zombie processes. Importantly, unlike the Bernstein and Gibson SYN cookie methods of the known art, in the Applicants' invention, TCP connection parameters are not limited to the least common denominator of client and server specified TCP connection parameters. Rather, in the present invention TCP connections can be established based upon client specified TCP connection parameters. Furthermore, even in the event of a SYN or ACK flood attack, TCP connection parameters can be selected for legitimate TCP connections according to a close approximation of selected parameters stored in a “blended SYN cookie”.

For example, in a method of the invention, a blended SYN cookie can be generated in a server in response to receiving a SYN request from a client. The blended SYN cookie can be stored in the low order bits of the server-selected packet sequence number field of a responsive SYN/ACK packet and can include a hash of the IP address of the server, the port of the server, a constant random seed and a date and time value. The blended SYN cookie further can include an index into a table of suitable TCP connection parameters and a client-selected packet sequence number. Notably, the table index can reference a particular set of TCP connection parameters which closely approximate, if not match, those TCP connection parameters specified by the client requesting the TCP connection with the server.

Thus, it will be apparent to the Examiner that the Applicants' invention addresses the deficiencies of prior art methods and systems including the Genesis and SYN cookie techniques of Bernstein discussed at length from line 19, page 3 to line 19, page 5 of the Applicants' specification. Specifically, in the Applicants' invention, not only are network servers immunized from SYN and ACK flood attacks, but also network servers are secure from attacks which bypass the TCP three-way handshake. Finally, the Applicants' invention permits both clients and servers to nominate a full range of session parameters and is not limited to the least common denominator of session parameters specified by the server.

Turning now to the rejections on the art, Watson relates to a system and method for validating a session request and transacting a communication session for a validated connection. In the Watson invention, an intermediary receives a session request from a requesting client. In response, a SYN cookie is generated and a session is opened only if the SYN cookie is properly acknowledged by the requesting client. Subsequently, a connection is initiated with a responding server and the session is transacted by translating sequence numbers by an offset reflecting the client versus the server sequence numbers. Finally, the session is terminated upon the request of either the client or server.

Notably, in the only portion of the Watson reference which addresses the use of SYN cookies, the Watson system and method indicate that the utilized SYN cookie methodology is that of Bernstein. Specifically, as stated in column 12, lines 21 through 24,

> **In the described embodiment, SYN cookies are generated using the technique described in D. Bernstein et al., "TCP SYN Cookies," http.//cr.yp.to/syncookies.html (1996), the disclosure of which is incorporated by reference.**

The Examiner will recall from the Applicants' specification, however, that Bernstein is deficient in that the SYN cookie of Bernstein does not allow for client specified communications parameters to be adopted by the server resulting in a lowest common denominator connection. Moreover, the SYN cookie of Bernstein permits the casual observer to decrypt the hash merely by observing a small sampling of valid traffic between the server and its clients. Moreover, Bernstein remains vulnerable to a "quasi-TCP" attack.

As claimed by the Applicants, several aspects of the inventive "blended SYN cookie" overcome the known deficiencies of Bernstein (and Watson by extension). First, the Applicants utilize an "index value into a table of pre-configured sets of communications sessions parameters, said index value referencing one of said sets which approximates said desired communications parameters". This claimed aspect of the invention is wholly lacking within the Watson reference. In fact, in column 12, lines 19 through 21 and lines 59 through 61, it is clear that the communications parameters used to establish a session with a requesting client are "the parameters for the current connection". Thus, Watson states exactly the opposite of what is claimed in claims 1, 8, 11 and 16. Second, Watson wholly lacks a reference to a "wrap around table" as in claims 3, 8 and 11. It is the "wrap around" feature, however, that allows the blended SYN cookie technique to remain impervious to a DoS flood attack as discussed in line 21, page 13 through line 2, page 14 of the Applicants' specification.

In sum, the Applicants believe that the originally filed claims 1-17 distinguish over the cited art and stand patentable and ready for an indication of allowance. As such, the Applicants respectfully request the withdrawal of the rejections under 35 U.S.C. § 102(e). This entire application is now believed to be in condition for allowance. Consequently, such action is respectfully requested. The Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: June 27, 2005

Steven M. Greenberg
Reg. No.: 44,725
Attorney for Applicant(s)
Christopher & Weisberg, P.A.
200 East Las Olas Boulevard, Suite 2040
Fort Lauderdale, Florida 33301
Customer No. 46320
Tel: (954) 828-1488
Fax: (954) 828-9122